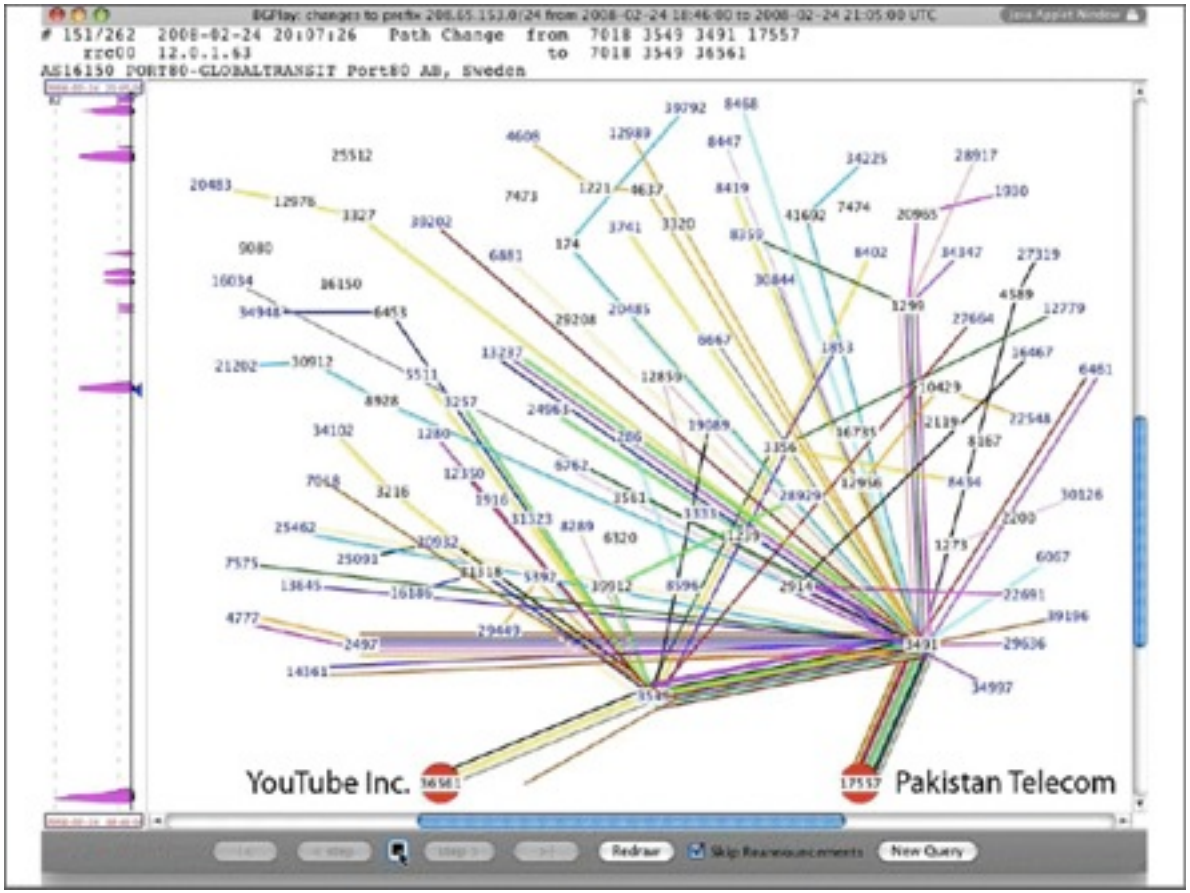
BGP Route Origin Validation

Mark Dranse <markd@ripe.net>
RIPE NCC

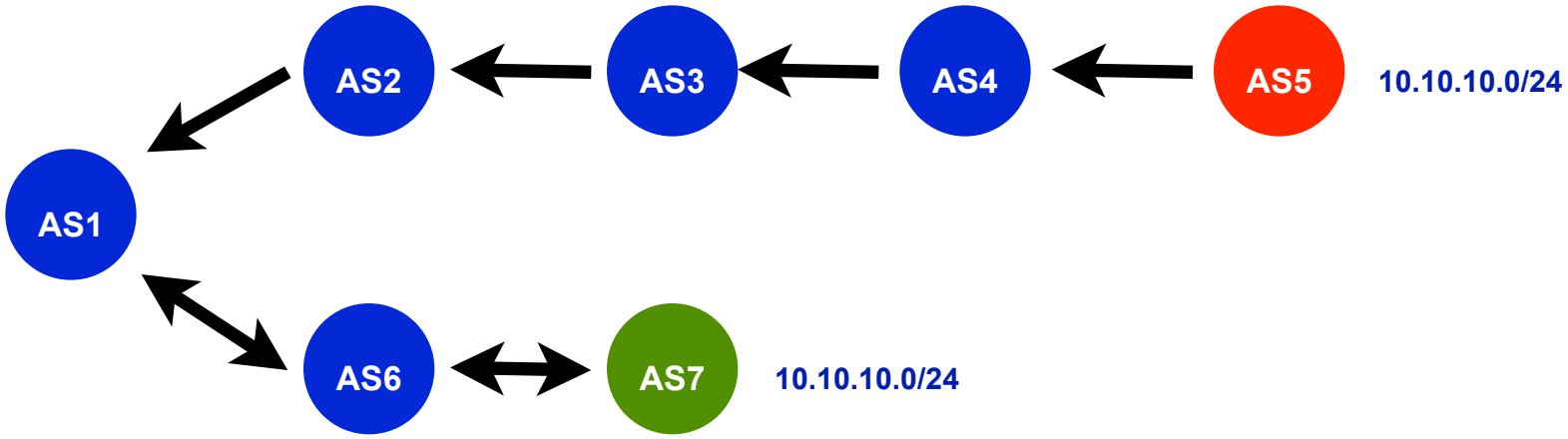
Background

- Routing infrastructure vulnerable to attacks
  - e.g. more specific routes (Pakistan Telecom vs Youtube)



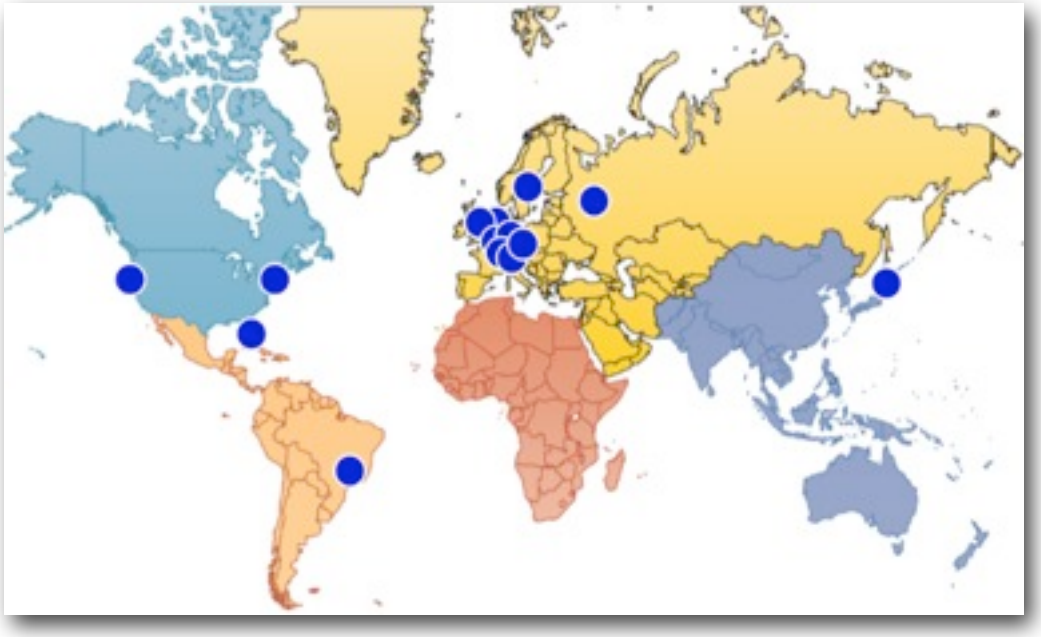
Background

- Routing infrastructure vulnerable to attacks
  - announce someone else's prefix
  - shortest AS-path wins



Source Data

- Routing Information Service (RIS)
  - 15 Remote Route Collectors
  - 600+ peers globally
  - 10 years of data



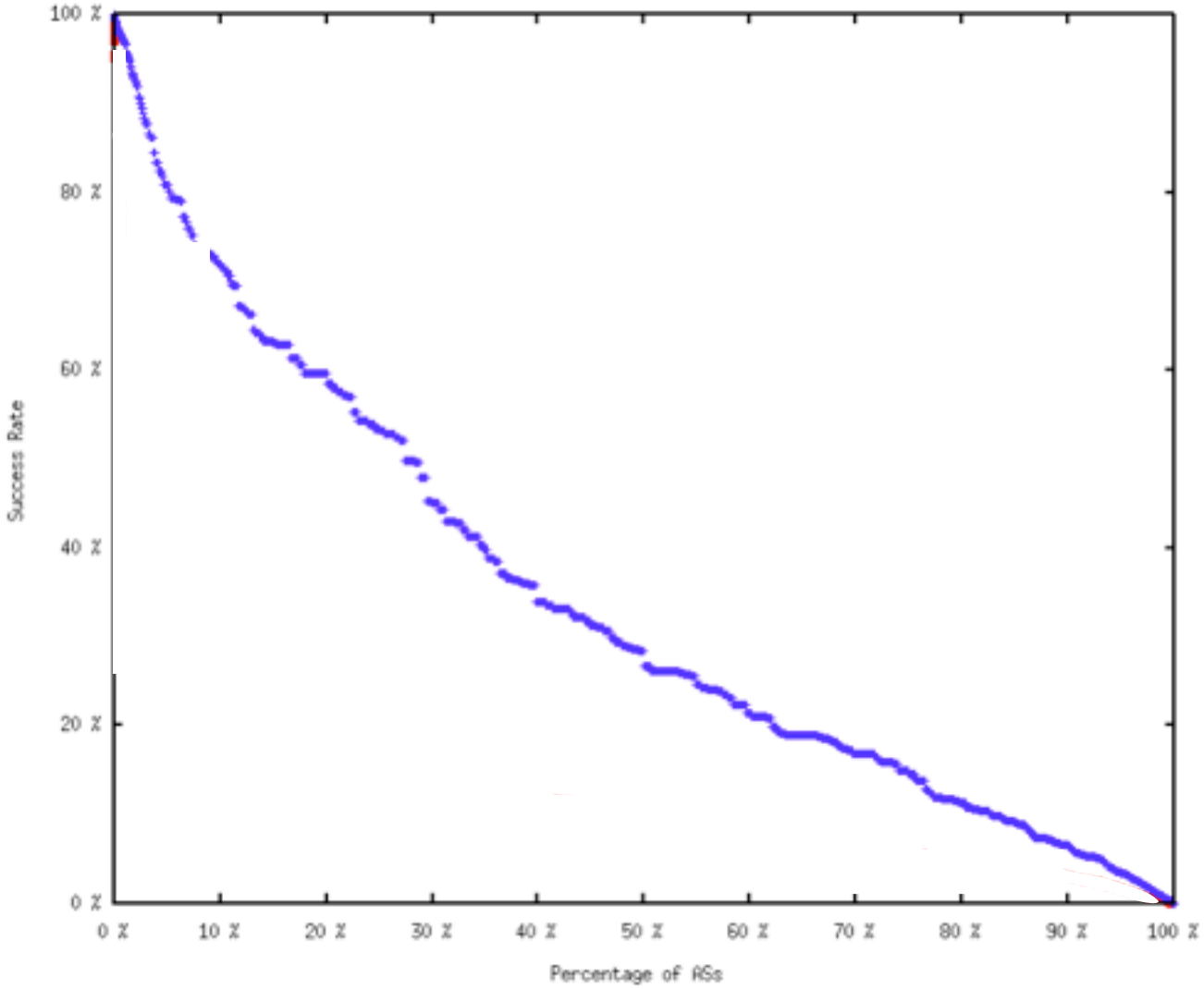
http://is-portal.ripe.net/

Methodology

- Take RIS data for all full table peers (82)
- Estimate when bogus routes are preferred
  - Ignoring ROAs
  - With every AS as attacker and target
  - ~35,000^2 combinations

34.2%

Mean hijack success per peer

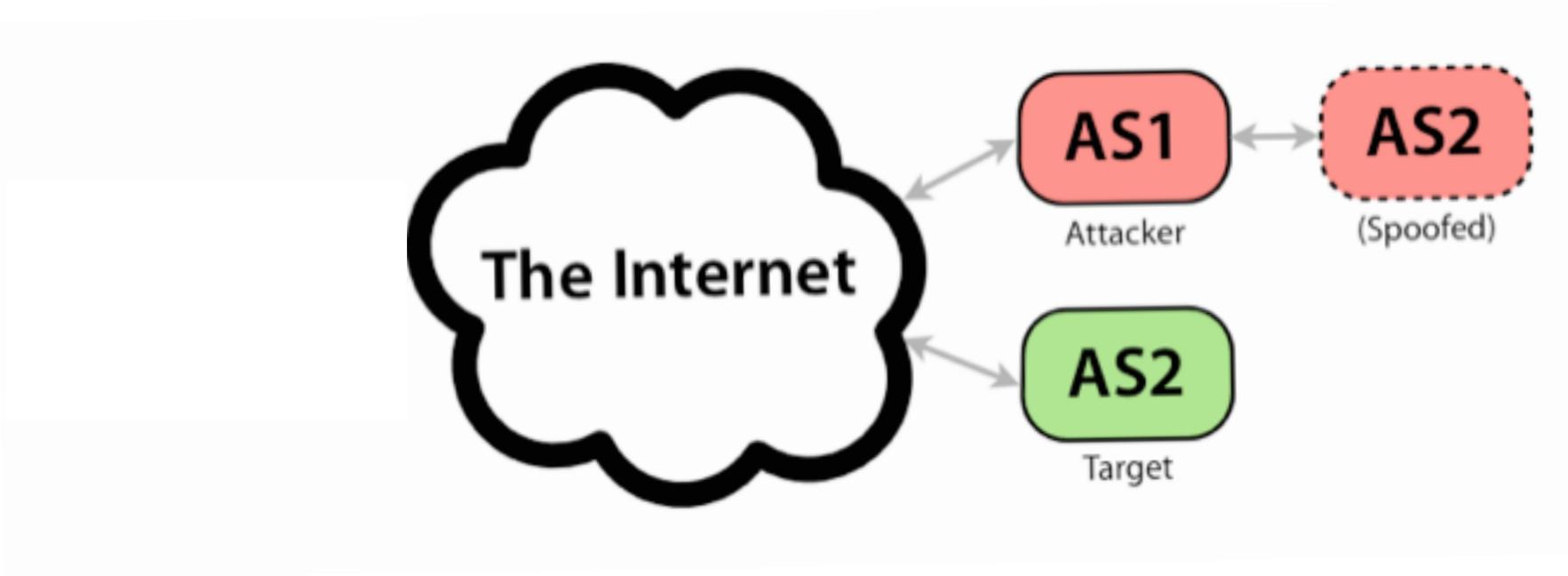


Mitigation

- Can be mitigated by RPKI
  - Used to certify Internet Number Resources
  - And inject this into routing policy creation
- RPKI supports *Origin Validation*
  - Checks if an AS can announce a specific prefix
  - But: can be attacked with *spoofed origin prepending*
- RIPE NCC examined possible success of this
  - Credit to David Murray, Information Services group

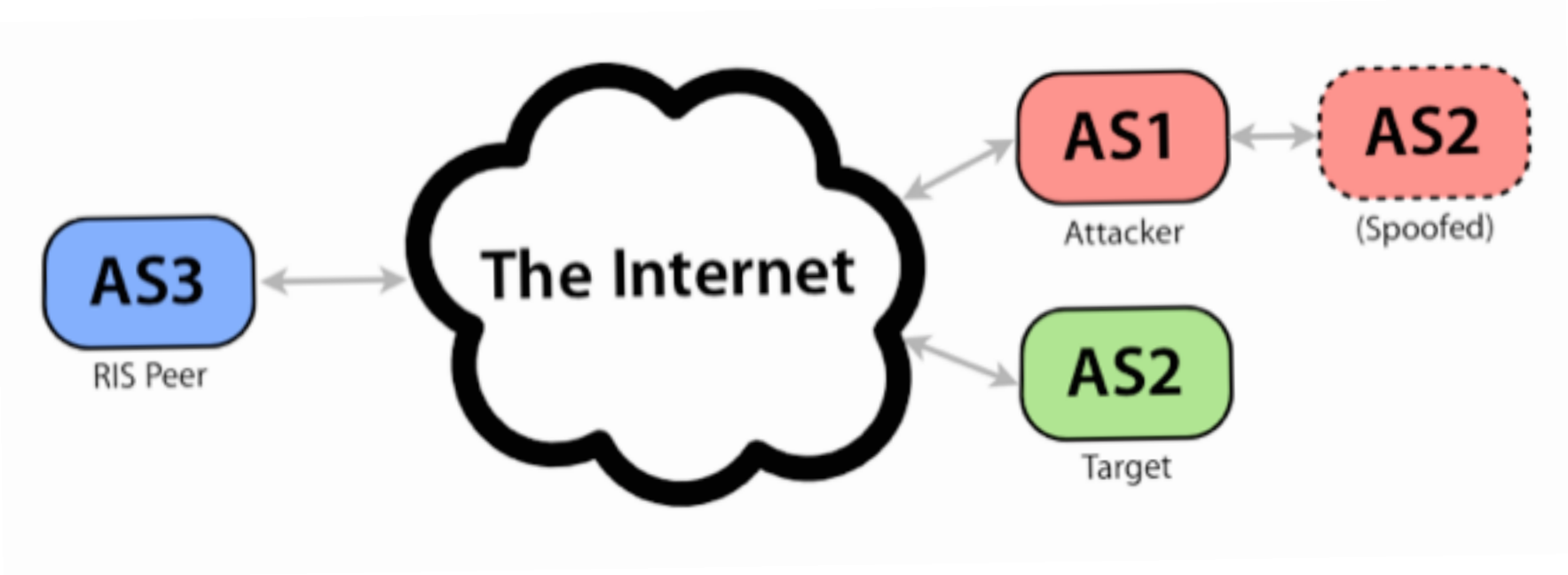
Attack

- Prepend valid origin to fraudulent route
- e.g. AS1 wants to hijack a prefix from AS2
  - Announce with AS2 as spoofed origin
  - Transit through AS1 network



Attack

- Prepend valid origin to fraudulent route
- e.g. AS1 wants to hijack a prefix from AS2
  - Announce with AS2 as spoofed origin
  - Transit through AS1 network



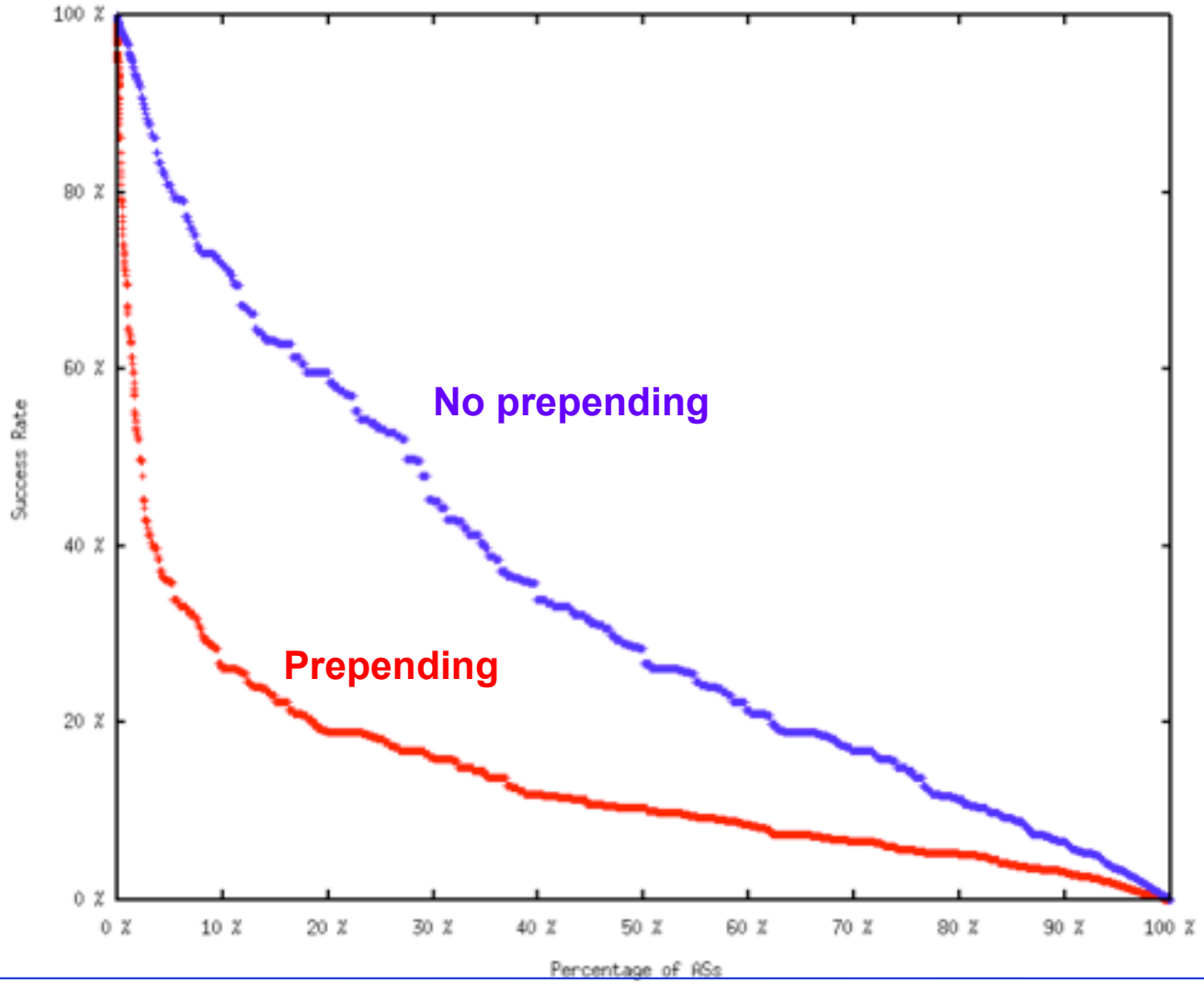
Methodology

- Take RIS data for all full table peers (~90)
- Estimate when prepended routes are preferred
  - With every AS as attacker and target
  - ~35,000^2 combinations

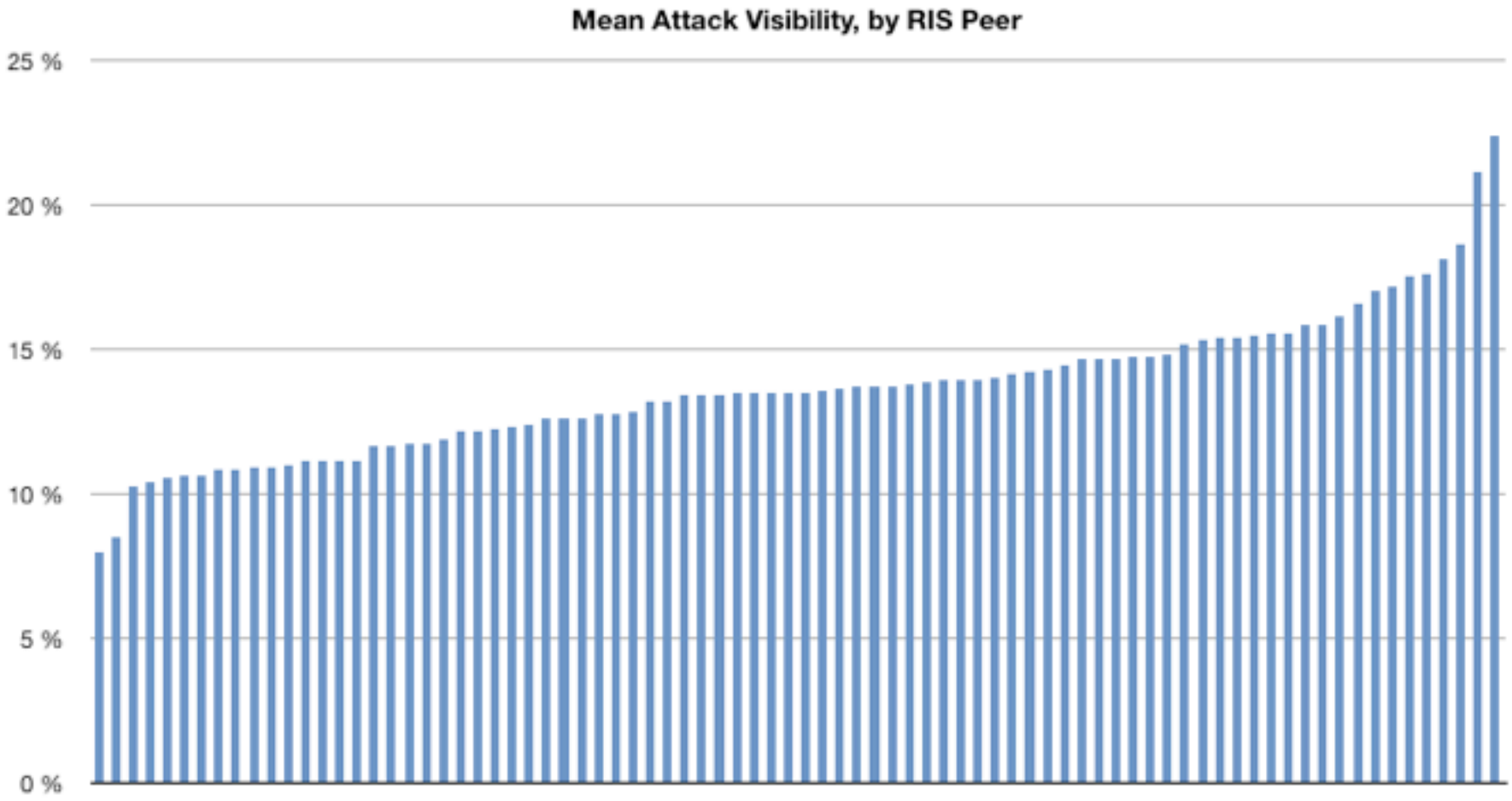
~~34.2%~~ **13.6%**

- This varies from 7%-22% depending on the AS

Mean hijack success per peer



Susceptibility per peer



Observations

- Assumes 100% route origin validation
  - Real deployment probably less
- Assumes shortest path wins
  - Other factors at play
- Limited dataset (82 full tables)
  - Representative but not comprehensive view
- Significant drop in success with longer path
- Can be solved with path validation

http://labs.ripe.net

Questions?